

2. 椭圆曲线上的 J -函数与 L -函数.

有限域上的代数曲线

$V: \mathbb{F}_p$ 上的光滑射影代数簇.

定义 V_{rep} 的 ζ -函数为:

$$Z(V, T) = \exp\left(\sum_{m \geq 1} |V(\mathbb{F}_p^m)| \cdot \frac{T^m}{m}\right) \in \mathbb{Q}[[T]]$$

$$\zeta(V, s) := Z(V, p^{-s}) \quad (s \in \mathbb{C}) \quad (\text{局部 } \zeta\text{-函数})$$

Weil Conjecture (Deligne Fields I of)

- ① $z(V, T)$ 是关于 T 的有理函数 $\in \mathbb{Q}(T) \subseteq \mathbb{Q}[[T]]$

- ② $\zeta(V, s)$ 有關於 $\operatorname{Re}(s) = \frac{n}{2}$ 對稱函數級. $s \leftrightarrow n-s$

$$\zeta(v, s) = \zeta(v, n-s) \cdot \boxed{??}$$

- ③ $\mathcal{I}(V, \omega)$ 的零点的实部是某些半整数

Wait的思路: 对下上代码建立一套与微分流列上的操作相类似的上同

调理论. (原由 Grothendieck 建立: étale 上同调), 但反对 Frobenius 映射 "Frob: $X \rightarrow X^q$ " 用 Lefschetz 不动点定理的类比物.

(F_{rob} 的不动点正是 $F_{rob}: \overline{\mathbb{F}_p} \rightarrow \overline{\mathbb{F}_p}$ $\overline{\mathbb{F}_p}^{F_{rob}} = \mathbb{F}_p$
 $x \mapsto x^p$
 $V(\overline{\mathbb{F}_p})^{F_{rob}} = V(\mathbb{F}_p)$ 正是 $Z(V, T)$ 中的
 某些系数)

而曲度级来源于 Poincaré 对偶.

例. $V = P^0_{TF}$ 为 Hz / T_F $Z(V, T)$

$$\log Z(\mathbb{P}^0_{\pi_P}, T) = \sum_{m \geq 1} 1 \cdot \frac{T^m}{m} = \log \frac{1}{1-T}$$

$$\text{若 } s = \sigma + it$$

$$|\rho^s| = p^\sigma$$

$\zeta(E, s)$ 的零点的实部

$$\sigma = \frac{1}{2} \Leftrightarrow |\alpha| = |\beta| = p^{\frac{1}{2}}$$

$$(1-\alpha T)(1-\beta T) = 1 + a_p T + p T^2$$

若 $a_p^2 - 4p \leq 0$ 则 α, β 为复数

$$\text{又 } \alpha \cdot \beta = p \text{ 故 } |\alpha| = |\beta| = p^{\frac{1}{2}}$$

反之, 若 $|\alpha| = |\beta| = p^{\frac{1}{2}}$, 则 $|\alpha + \beta| \leq |\alpha| + |\beta| = 2p^{\frac{1}{2}} = 2\sqrt{p}$

$$\text{从而 } |a_p| \leq 2\sqrt{p} \Leftrightarrow E/\mathbb{F}_p \text{ 上的 Riemann 假设}$$

Hasse-Wald $\uparrow$

exer 证明函数方程 $\zeta(E, s) = \zeta(E, 1-s)$

$\mathbb{Q}$ 上代数簇

$V/\mathbb{Q}$ 光滑射影代数簇 定义簇的系数 $\mathbb{Z}$, 可作 mod p 约化

若 $V/\mathbb{F}_p$ 仍光滑 $\zeta(V_p, s)$

对坏的 p 补充定义 $\zeta(V_p, s)$

$$\zeta(V, s) = \prod_p \zeta(V_p, s)$$

Riemann 假设 V_p 成立 (Deligne) $\Rightarrow \zeta(V, s)$ 在 $\text{Re}(s) > 1 + \dim(V)$ 这个半平面上无零点 $\prod_p$ 收敛.

(Lang (Hasse-Wald) $V/\mathbb{Q}$ 光滑代数簇 那么

$\zeta(V, s)$ 在 $\mathbb{C}$ 上可解析延拓为一个亚纯函数, 满足某个关于 $s \leftrightarrow d+1-s$ 对称的函数方程. (且零点的实部是某些有理数)

例 取 $V = \mathbb{P}^n_{/\mathbb{Q}}$ 所有 p 处均光滑

$$\zeta(V_p, T) = \frac{1}{1-T}$$

$$\zeta(V_p, T) = \frac{1}{1-p^{-s}}$$

Riemann 假设

$$\zeta(\mathbb{P}^n, s) = \prod_p \frac{1}{1-p^{-s}} = \sum_{n \geq 1} \frac{1}{n^s} = \zeta(s) \text{ 正是 Riemann } \zeta\text{-函数}$$

exer 对于 $V = \mathbb{P}^n_{/\mathbb{Q}}$ 求 $\zeta(\mathbb{P}^n, s) = \zeta(s) \cdot \zeta(s-1) \cdots \zeta(s-n)$

对于 $V = P_{\mathbb{A}}$ 有 $S(V, s) = s(s-1) \cdots s(s-n)$

$$V = \mathbb{Z} \quad \text{Weierstrass 形式}$$

$$\Delta_E \in \mathbb{Z}$$

$$p \nmid \Delta_E \Leftrightarrow p \nmid \text{disc } E$$

$$E_p/F_p \text{ 非平凡扩张} \quad \zeta(E_p, s) = \frac{1 - \alpha_p p^{-s} + p^{1-2s}}{(1-p^{-s})(1-p^{1-s})}$$

$$\zeta_s(E_p, s) = \prod_{p \nmid S} \zeta(E_p, s) = \frac{\zeta_s(s) \zeta_s(s-1)}{L_s(E, s)} \quad (s \in \mathbb{C})$$

$$E_p/F_p = S \subset \Omega_{\mathbb{A}}$$

$$\prod_p \zeta(E_p, s) = \prod_{p \nmid S} \frac{1}{1 - \alpha_p p^{-s} + p^{1-2s}} = \prod_{p \nmid S} \frac{1}{1 - \alpha_p p^{-s}} \cdot \frac{1}{1 - \beta_p p^{-s}}$$

$$|\alpha_p| = |\beta_p| = p^{\frac{1}{2}}$$

$$\text{Riemann } \zeta \text{ 中 } \prod_p \frac{1}{1 - p^{-s}} \text{ 在 } \operatorname{Re}(s) > 1 \text{ 收敛}$$

$$\text{从而 } \prod_p \frac{1}{1 - p^{\frac{1}{2}} \cdot p^{-s}} \text{ 在 } \operatorname{Re}(s) > \frac{3}{2} \text{ 收敛}$$

$$\text{故可得 } \prod_{p \nmid S} \frac{1}{1 - \alpha_p p^{-s}} \cdot \frac{1}{1 - \beta_p p^{-s}} \text{ 在 } \operatorname{Re}(s) > \frac{3}{2} \text{ 收敛}$$

最后对 $p \in S$ 不收敛时，补充定义

$$L_p(T) = \begin{cases} 1 - \alpha_p T + p T^2 \\ 1 - T \\ 1 + T \\ 1 \end{cases}$$

p 收敛

p 处条件收敛

p 处绝对收敛

~~$\times$~~ $\rightarrow$ 对 $p \in F_p$
 $\in F_p$

$$L_p(p^{-s}) = \begin{cases} 1 - \alpha_p p^{-s} + p^{1-2s} \\ 1 - p^{-s} \\ 1 + p^{-s} \\ 1 \end{cases}$$

$$\text{当 } s=1 \text{ 时 } L_p(p^{-1}) = \frac{|E_p^\circ(F_p)|}{p}$$

$$E_p^\circ = E_p \setminus \text{不收敛点}$$

$$L_s(E, s) = \prod_{p \nmid S} \frac{1}{L_p(p^{-s})}$$

$$L(E, s) = \prod_{p \in S_Q} \frac{1}{L_p(p^{-s})}$$

无穷级 $v=\infty$ 上 L_∞ 是一些 Γ 函数.

$$\Lambda(E, s) = \underbrace{N_{E/Q}^{\frac{s}{2}} (2\pi)^s \Gamma(s)}_{\text{Conductor}} \cdot L(E, s)$$

Hasse-Weil Conj :

$\Lambda(E, s)$ 在 $\mathbb{C}$ 上可解析延拓为一个互值函数, 满足函数方程
 $\Lambda(E, s) = w_E \Lambda(E, 2-s)$ (其中 $w_E = \pm 1$)

Thm (Wiles, Breuil-Coleman-Diamond-Taylor)

对 E/Q (半稳定) 都有同构上述 Conj 成立!

Rh. (他证明了) Taniyama-Shimura-Weil Conj: $L(E, s)$ 与一个模形式 L 函数是一样.

模椭圆曲线.

解析对象
 $\downarrow$
 L -函数性质很好

3. Fermat 大定理

$$x^n + y^n = z^n \quad (n \geq 3)$$

$$E: y^2 = x(x-a^n)(x+b^n) \quad (\text{若 } a \neq 0, b \neq 0, a \neq \pm b \text{ 则 } \Delta \neq 0)$$

(Frey 构造).

Frey 1982-1985:

发现 (反例) 若 $a, b \in \mathbb{Q}$ 且 $a^n + b^n = c^n$ ($n \geq 3$) $\mathbb{Q} \subset \mathbb{C}$

那么 E 的 L -函数将不可能是一个模形式!

Serre 85 + Ribet 86 证明了 Frey 的猜想:

即只要 $a^n + b^n = c^n$ 则 Frey 曲线与 Taniyama - Shimura - Weil 猜想矛盾.

Wiles: 证明了半稳定的 $E/\mathbb{Q}$ T-S-W 成立! $\Rightarrow$ Fermat 大定理 $\checkmark$.

4. BSD 猜想

$$K = \mathbb{Q} \quad E: y^2 = x^3 + ax + b$$

$$\omega = \frac{dx}{2y}$$

$E(\mathbb{Q})/E(\mathbb{Q})_{\text{tor}}$ 有一组 $\mathbb{Z}$ -基 $P_1, \dots, P_r$

Néron-Tate 高度 $\leadsto$ 内积 $(E(\mathbb{Q}) \otimes \mathbb{R}) \times (E(\mathbb{Q}) \otimes \mathbb{R}) \rightarrow \mathbb{R}$
 $P, Q \mapsto \langle P, Q \rangle$

$$\text{Reg}(E/\mathbb{Q}) = \det(\langle P_i, P_j \rangle)_{1 \leq i, j \leq r}$$

(regulator)

Conj (Birch - Swinnerton-Dyer)

(1) $L(E, s)$ 于 $s=1$ 处零点的阶数为 $r = \text{rk } E(\mathbb{Q})$

(2) $\lim_{s \rightarrow 1} \frac{L(E, s)}{(s-1)^r} = \Omega \cdot \underbrace{(\prod_p c_p)}_{\neq 0} \cdot \frac{|L(E/\mathbb{Q})| \text{Reg}(E/\mathbb{Q})}{|E(\mathbb{Q})_{\text{tor}}|^2}$ 对于 $E/\mathbb{Q}$ 均成立

其中 $\Omega = \int_{E(\mathbb{R})} |\omega|$

$c_p = [E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)]$ 依赖于环的局部信息

$$E^0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) = E(\mathbb{Z}_p) \mid P \text{ 的阶化不是那个不整的数}\}$$

事实上: $\frac{c_p \cdot |E^0(\mathbb{F}_p)|}{p} = \int_{E(\mathbb{Q}_p)} |\omega|$
 Haar 测度.

可于代数数论中类似公式证明:

Th (类似公式) K : 数域 (则 $\zeta_K(s)$ 于 $s=1$ 处有单重极点)

$$1. \quad (a+1)(a-1) = 2^{r_1} (2a)^{r_2} \text{Res}_{s=1} \zeta_K$$

1.1 (2.2.2.2) $K = \mathbb{Q}(\sqrt{D_K})$ $D_K \equiv 1 \pmod{4}$ or $D_K \equiv 0 \pmod{4}$

$$\lim_{s \rightarrow 1} (s-1) \zeta_K(s) = \frac{2^{r_1} (2\pi)^{r_2} \text{Reg}_K \cdot h_K}{w_K \cdot \sqrt{|D_K|}}$$

r_1 : K 的实嵌入个数

r_2 — 复 — 嵌入 — 个数 —

Reg_K : regulator 由 $O_K^\times$ 的值给出

$h_K = |\text{cl}(K)|$ 类群的阶

$$w_K = |(O_K^\times)_{\text{tor}}| = |\mu(K)|$$

D_K 为 $K/\mathbb{Q}$ 的 discriminant.

已知的一些结果:

Gross-Zagier (1986): 若 $E/\mathbb{Q}$ 为 ~~模椭圆曲线~~ 且 $L(E, s)$ 在 $s=1$ 处有一阶零点, 则 $\text{rk } E(\mathbb{Q}) \geq 1$

Kolyvagin (1989): $E/\mathbb{Q}$ 模椭圆曲线. 若 $L(E, 1) \neq 0$ 则 $\text{rk}(E(\mathbb{Q})) = 0$.
若 $L(E, s)$ 在 $s=1$ 处一阶零点, 则 $\text{rk } E(\mathbb{Q}) = 1$.
即 BSD (1) $\checkmark$.

Bhargava-Shankar (2015): $E/\mathbb{Q}$. 则秩的平均值 $\leq \frac{7}{6}$

(Conj: 平均值为 $\frac{1}{2}$, 一半 $\text{rk}=0$, 一半 $\text{rk}=1$, 其他 conjecture 没有)

$\Rightarrow$ 有一个正比例的 $E/\mathbb{Q}$, $L(E, 1) \neq 0$ 从而由 Kolyvagin
+ 其他的结果 BSD (1) $\checkmark$.

BSD 的一个应用

同余数问题:

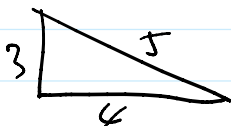
Def $n \in \mathbb{N}$ n 无平方因子, 称 n 为 同余数, 若它是一个三边为有理数的
有内角三角形的面积.

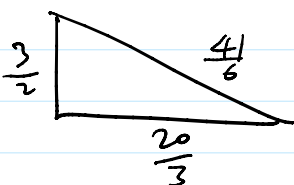
$r \in \mathbb{Q}$ (非0) 同余数

Rh. $\forall r \in \mathbb{Q}, r > 0$ 总有 $s \in \mathbb{Q}^+$ $r \cdot s^2 \in \mathbb{N}$ 且无平方因子,

Rh. $\forall r \in \mathbb{Q}, r > 0$ 总存在 $s \in \mathbb{Q}^+$ $r \cdot s^2 \in \mathbb{N}$ 且无平方因子,
 $r \cdot s^2$ 为同余数 $\Leftrightarrow r$ 为同余数

(古希腊): 同余数问题: 给定 $n \in \mathbb{N}$, 是否可判断 n 为同余数?

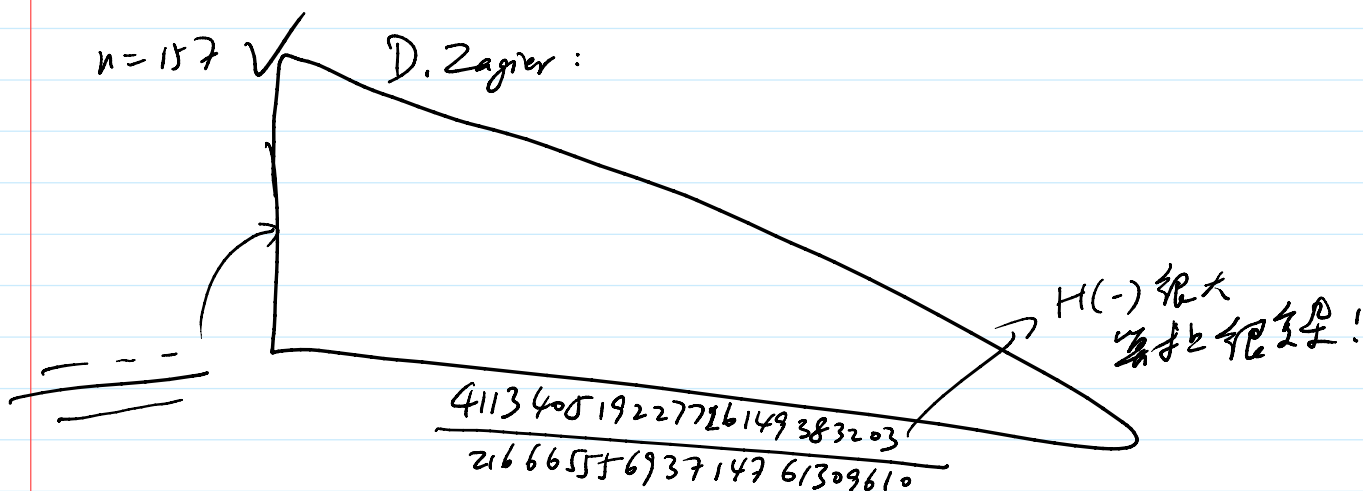
例. $n=6$ $\checkmark$. 

非同余数: $n=5$ $\checkmark$ 

Euler: $n=7$ $\checkmark$ $(\frac{24}{5}, \frac{35}{12}, \frac{337}{60})$

Fermat: $n=1$ 不是同余数. ($\Leftrightarrow x^4 + y^4 = z^4$ 无解)

$n=157$ $\checkmark$ D. Zagier:



Th (Tunnell) $n \in \mathbb{N}$ 无平方因子, 奇数:

(A) n 是同余数

$$\boxed{(B)} \left| \{ (x, y, z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 8z^2 = n \} \right| = 2 \left| \{ (x, y, z) \in \mathbb{Z}^3 \mid 2x^2 + y^2 + 32z^2 = n \} \right|$$

那么 $A \Rightarrow B$ 而且 $B \xrightarrow{\text{BSD}} A$

exer 对 $n=157$ 验证 B.

cf. GTM 97. Koblitz: Introduction to Elliptic curves and Modular Forms.

$$\begin{array}{c} z \\ \backslash \\ n \\ / \\ x \end{array} \quad n \text{ 为偶数}$$

$\Updownarrow$ (初等数论)

$$E_n: y^2 = x^3 - n^2x \quad \text{有无无穷 } \mathbb{Q}\text{-点, 即 } \text{rk } E_n(\mathbb{Q}) \neq 0$$

$\Downarrow$ Coates-Wiles

$\Uparrow$ BSD

$L(E_n, s)$ 于 $s=1$ 处为正则

$\Updownarrow$ Shimura + Waldspurger + Tunnell

Tunnell 构造的基类 θ -函数 (一种模形式)
的 q -展式的第 n 个系数为 0

